

## REMARKS

Claims 29-42 were presented for examination and were pending in this application. In an Official Action dated September 23, 2003, claims 29-42 were rejected. Applicants thank Examiner for examination of the claims pending in this application and addresses Examiner's comments below. Applicants also thank Examiner for the Examiner Interview granted on February 12, 2004. In accordance with 37 CFR § 1.133 and MPEP § 713.04, the substance of the interview is incorporated herein.

Applicants herein amends claim 29 to delete the word "and" after the clause "comparing a predetermined parameter associated with the user with a pre-determined parameter associated with the data to determine permission to access the data." This change does not introduce new matter, and entry is respectfully requested. The claim has been amended to expedite the prosecution of the application in a manner consistent with the Patent Office Business Goals, 65 Fed. Reg. 54603 (Sept. 8, 2000). In making this amendment, Applicants have not and do not narrow the scope of the protection to which Applicants consider the claimed invention to be entitled and do not concede that the subject matter of such claims was in fact disclosed or taught by the cited prior art. Rather, Applicants reserve the right to pursue such protection at a later point in time and merely seek to pursue protection for the subject matter presented in this submission.

In addition, Applicants note that new claims 43 to 48 have been added. Support for these claims is found throughout the specification, for example, at pages 10 through 12 and Figures 2 through 4.

**Response to Rejection Under 35 USC 102(b)**

In the 2nd and paragraph on page 3 of the Office Action, Examiner rejects claims 29-30, 36, 38, and 42 under 35 USC § 102(b) as allegedly being anticipated by U.S. Patent Application Publication No. 20020133412 to Oliver et al. (“Oliver”). This rejection is now traversed.

Representative claim 29 recites, in part, a method:

for use in a detector device for controlling access to information on a network including a plurality of interconnected devices, the detector device coupled to the network between a first device and a second device, the method comprising:

monitoring a plurality of request signals for data between the first device and the second device in the network, at least one request signal including a user identification parameter;

in response to an operational failure within the detector device, allowing the plurality of request signals to pass uninterrupted between the first device and the second device.

The claimed invention beneficially provides a method for use in a detector device coupled between a first and a second device and monitoring request signals between the devices. Further, the process includes providing for a response to a request signal from, e.g. the first device while also allowing for the detector device to continue passing request signals between the first device and second device when there is an operational failure. Thus, the claimed invention provides monitoring and response processes without introducing a point of failure between two communicating devices on a network and without requiring integration with entities that control either device or requiring a formal reporting structure with the entities owning either device. Oliver fails to disclose (or suggest) the claimed invention.

Oliver discloses system that requires websites to provide their own authentication services; Oliver's validation server only provides user profile and class information to a website if a website sends a token to the validation server:

[I]ndividual publishers or service providers *authenticate their own users*, and then ask TVS to store the user's preference, pricing and service-class information in a 'publicly accessible' place. In return, *TVS provides an authentication token* which is returned to the user.... All subsequent access to any TVS-enabled service is governed by this token (non-TVS services are not affected). TVS validates the token on behalf of any individual service, *and passes in return the user's profile and class information*. (Emphasis added).

*Oliver*, ¶ 114.

The claimed invention, unlike Oliver, operates within a detector device located between a first device, e.g., a user, and a second device, e.g., website server. The detector device in Oliver is the CALS shown in Figure 2 and described in paragraph 39:

CLICKSHARE SERVICE CORP.--Facilitating the authentication of Clickshare Users, and storing records of their access to web sites is the Clickshare Access and Logging Service (CALS). Operated by Clickshare Service Corp. or its licensees, CALS is a fault-tolerant network of one or many Internet servers which exchange real-time, encoded information with machines operated by information sellers and billing agents.

*Id.*, ¶ 39. This CALS system is not located between a first device, i.e., the CMa end-user system, and a second device, i.e., the CSPa server system. *See Id.*; *See also, Id.*, ¶ 149, 306-310, 344, 347, 373 (location of structures and operation of system). Rather, the CALS system is located behind the server CSPa, i.e., the back-end of the system. The reason the CALS system is on the back-end is because it controls access to the CSPa server in terms of whether or not to grant access to the end user-system CMa so CMa can establish a connection with the server CSPa. In particular, Oliver notes that:

If the CM is found to be properly authorized, CSPa's TVS-enhanced server daemon employs a pre-established UDP connection to its CALSa to (a) Submit user-profile information to CALSa for storage in the CALSa dynamic session database; and (b) Direct CALSa to issue

and return via UDP a globally unique session token. This token is also stored in the CALSa dynamic session database and is referenced to the related user-profile information also contained there.

*Id.*, ¶ 344. This passage specifically discloses that the CALS system is on the back end of the CSPa server and not coupled between the CSPa and CM devices. Hence, Oliver does not disclose a detector device coupled between a first device and a second device in a network for processing requests between them in a manner as claimed by Applicants.

In addition, Applicants also note that Oliver does not disclose a system for providing operation without introducing a point of failure as claimed by Applicants. Specifically, Oliver does not disclose “in response to an operational failure within the detector device, allowing the plurality of request signals to pass uninterrupted between the first device and the second device” as Applicants claim. Rather, Oliver does disclose a fail over mechanism, for example, in ¶ 327. However, this fail-over system operates as follows:

Since the TVS service is provided on machines separate from the HTTP servers, there is a possibility that either machine failure or network outage may make the service unavailable temporarily. In such cases, the HTTP server will issue itself a “restart” which will attempt to reconnect the server to another TVS server on another part of the network. Users with active sessions will have to re-authenticate with their home publisher, but this is transparent given graceful handling by the TVS client web server and caching of username/password in most browsers.

*Id.*, ¶ 263 (Emphasis added). This passage shows that the CALS system in Oliver is actually a point of failure. Its failover mechanism while providing availability, still introduces the CALS system as a point of failure because it requires interrupting communications between the CMa and CSPa to allow for reconnecting with another server and having a user system go through a re-authentication process to reconnect. Hence, this system actually teaches away from Applicants’ claimed invention of “in response to an operational failure within the detector device, allowing the plurality of request signals to pass uninterrupted between the first device and the second device.”

Therefore, for at least the reasons set forth above, Applicants respectfully submit that Applicants claimed invention is patentably distinguishable over the Oliver reference. Applicants respectfully request withdrawal of the basis of the rejection and allowance of this claim.

In addition, the reasoning set forth above with respect to claim 29, also applies to claims 30, 36, 38, and 42 and is incorporated herein by reference. Therefore, Applicants respectfully request withdrawal of the basis of the rejection and allowance of these claims.

**Response to Rejection Under 35 USC 103(a) in View of Oliver et al. and Iwamura**

In the 5<sup>th</sup> paragraph on page 5 of the Office Action, Examiner rejects claims 31-32, 35, 37, and 39-40 under 35 USC § 103(a) as allegedly being unpatentable in view of Oliver and U.S. Patent No. 6,272,535 to Iwamura. (“Iwamura”). This rejection is respectfully traversed.

Claims 31, 32, and 35 depend from claim 29 and claims 37, 39 and 40 depend from claim 36. The arguments set forth above regarding claims 29 and 36 being distinguishable over Oliver are applicable to these claims and are herein incorporated by reference. Therefore, Applicants respectfully request withdrawal of the basis of the rejection and allowance of these claims.

In addition, Applicants note that Iwamura is also a deficient reference with respect to these claims. For example, claim 31 recites “allowing access to the data when the predetermined parameter associated with the user is less than or equal to a predetermined parameter associated with the data.” However, Iwamura does not disclose a detector device that includes this process as claimed. Iwamura discloses allowing access to data when the predetermined parameter associated with the user is less than or equal to predetermined parameter associated with the data. *See, e.g., Iwamura, Abstract.* Moreover, Iwamura

clearly discloses that this calculation occurring at the user terminal. Specifically, it states that “[t]he user cannot actually obtain access to the downloaded information PP until the check circuit 14 determines that access is to be permitted.” *Id.*, 5:29-32. The referenced check circuit 14 is located in the user terminal. *See Id.*, FIG. 3.

Further, Iwamura requires the user terminal to be specialized. *See Id.*, 4:50-52 (“each terminal is provided with an accounting apparatus (See FIG. 3) which can communicate with the charge provider 18.”). By contrast, the claimed invention requires no such modification to any devices as it simply can be inserted into a network in an unintrusive manner between a first device and a second device.

Nor does the combination of Oliver and Iwamura disclose or suggest a process in a detector device as claimed. The combination discloses, at best, a back end detector device (as in Oliver) in which a user system, having installed on it an accounting apparatus, determines whether a threshold value is reached for getting access (as in Iwamura). This is not Applicants’ claimed invention in claim 31, in which a detector device between a first and a second device includes a process that “allow[s] access to the data when the predetermined parameter associated with the user is less than or equal to a predetermined parameter associated with the data.”

Hence, for at least the reasons set forth above, Applicants respectfully submit that Applicants claimed invention in claim 31 is patentably distinguishable over both the Oliver and Iwamura references. Applicants respectfully request withdrawal of the basis of the rejection and allowance of this claim.

Moreover, similar reasoning with respect to the deficiencies of Oliver and Iwamura apply to the other claims 32, 35 37, 39 and 40, and the general arguments regarding these

deficiencies are incorporated by reference. Thus, Applicants respectfully request reconsideration of the basis for the rejection to these claims and allowance at this time.

### Conclusion

Applicants' have added new claims 43-48 for which Applicants request consideration and examination. Applicants respectfully submit that these are supported by the specification as noted above and are commensurate within the scope of protection to which Applicants' believe they are entitled.

In sum, Applicants respectfully submit that claims 29 through 42 as presented herein, are patentably distinguishable over the cited references (including references cited, but not applied). Therefore, Applicants request reconsideration of the basis for the rejections to these claims and request allowance of them.

In addition, Applicants respectfully invite Examiner to contact Applicants' representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,  
Stanislav Khirman, Mark Ronald Stone,  
Oren Arial and Ori Cohen

Date: 19 February 2004 By:

  
Rajiv P. Patel

Rajiv P. Patel, Attorney of Record  
Registration No. 39,327  
FENWICK & WEST LLP  
801 California Street  
Mountain View, CA 94041  
Phone: (650) 335-7607  
Fax: (650) 938-5200  
Email: rpatel@fenwick.com